A divisibility criterion for exceptional APN functions

Florian Caullery

A divisibility criterion for exceptional APN functions

Florian Caullery

Abstract. We are interested in the functions from $\mathbb{F}_{2^m}$ to itself which are Almost Perfectly Nonlinear over infinitely many extensions of $\mathbb{F}_2$, namely, the exceptional APN functions. In particular, we study the case of the polynomial functions of degree $4e$ with e odd and we give a necessary condition on an associated multivariate polynomial for the function to be exceptional APN. We use this condition to confirm the conjecture of Aubry, McGuire and Rodier in some new cases.

1. Introduction

A vectorial Boolean function is a function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. It is well known that all those functions admit a polynomial representation. Throughout this paper, we will refer to f as a function as well as a polynomial. These objects arise in fields like cryptography and coding theory and are of particular interest in the study of block-ciphers using a substitution-permutation network (SP-network) since they can represent a Substition Box (S-Box). In 1990 Biham and Shamir introduced the differential cryptanalysis in [**3**]. The basic idea is to analyze how a difference between two inputs of an S-box will influence the difference between the two outputs. This attack was the motivation for Nyberg to introduce the notion of Almost Perfectly Nonlinear (APN) function [**22**] which are the function providing the S-Boxes with best resistance against differential cryptanalysis. An APN function is a vectorial Boolean function such that $\forall a \neq 0, b \in \mathbb{F}_{2^m}$ there exist at most two solutions to the equation:

$$f(x + a) + f(x) = b.$$

A complete classification of APN function is an interesting open problem that has been widely studied by many authors. A first approach toward the classification was to consider only power functions and the studies was recently extended to polynomial functions (Carlet, Pott and al [**8, 14, 15**]) or polynomials on small fields (Dillon [**12**]). On the other hand, several authors (Berger, Canteaut, Charpin, Laigle-Chapuy [**2**], Byrne, McGuire [**7**] or Jedlicka [**5**]) showed that APN functions cannot exist in certain cases. Some also studied the APN functions on fields of odd characteristic (Leducq [**19**], Pott and al. [**13, 23**], Ness, Helleseth [**21**] or Wang, Zha [**27, 28**]).

1991 *Mathematics Subject Classification.* Primary 11C08, 11T06, 11T71.

Key words and phrases. vector Boolean functions, almost perfect nonlinear functions, algebraic surface, CCZ-equivalence, Gold function, Kasami function, exceptional number.

One way to face the problem of the classification is to consider the function APN over infinitely many extensions of $\mathbb{F}_2$, namely, the exceptional APN functions. The two best known classes of exceptional APN functions are the Gold functions: $f(x) = x^{2^i+1}$ and the Kasami functions $f(x) = x^{4^i-2^i+1}$, both are APN whenever i and m are coprime. We will refer to $2^i + 1$ and $4^i - 2^i + 1$ respectively as the Gold and Kasami exponent. Hernando and McGuire proved that those two functions are the only monomial exceptional APN functions [**17**]. It was the starting point for Aubry, McGuire and Rodier to formulate the following conjecture:

Conjecture 1 ([**1**]). The only exceptional APN functions are, up to Carlet Charpin Zinoviev-equivalence (as defined below), the Gold and Kasami functions.

We provide the definition of the Carlet Charpin Zinoviev equivalence:

Definition 1.1 ([**8**]). Two functions f and g are Carlet Charpin Zinoviev (CCZ-)equivalent if there exist a linear permutation between their graphs (i.e. the sets $\{x, f(x)\}$ and $\{x, g(x)\}$).

It is worth pointing out that all the functions CCZ-equivalent to an APN function are also APN [**8**].

By means of a simple rewriting of the definition of APN function in terms of algebraic geometry, Rodier was able to prove that, if the projective closure of the surface X defined by the equation:

$$\frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(y + z)(z + x)} = 0$$

has an absolutely irreducible component defined over $\mathbb{F}_{2^m}$, then f is not an exceptional APN function [**24**]. We will denote by $\bar{X}$ the projective closure of X. From now on we let $q = 2^m$,

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(y + z)(z + x)},$$

$$\phi_i(x, y, z) = \frac{x^i + y^i + z^i + (x + y + z)^i}{(x + y)(y + z)(z + x)}.$$

and

$$A = (x + y)(y + z)(z + x).$$

Writing $f = \sum_{i=0}^{d} a_i x^i$ with d the degree of f, we have $\phi = \sum_{i=0}^{d} a_i \phi_i$ and so the homogeneous equation of $\bar{X}$ is given by

$$\varphi(x, y, z, h) = \sum_{i=0}^{d} a_i \phi_i h^{d-i}.$$

The idea is to use the fact that if $\bar{X} \cap H$, where H is an hyperplane, has a reduced absolutely irreducible component then $\bar{X}$ has an absolutely irreducible component (see [**1**]). We wish to exploit this criterion to prove that the functions which are not CCZ-equivalent to a Gold or Kasami monomial are not exceptional APN. This approach enabled Aubry, McGuire and Rodier to state, for example, that there is no exceptional APN function of degree odd not a Gold or Kasami exponent as well as functions of degree $2e$ with e an odd number [**1**].

The next step was to study the polynomials of degree $4e$. Under the assumption that ϕ_e is absolutely irreducible, Rodier proved that an exceptional APN function should have its associated polynomial ϕ divisible by another polynomial with a specific form (see [**25**]). In the same paper, he treated the case of exceptional APN function of degree 12. It was later showed in [**10**] that there is no exceptional APN polynomial functions of degree $4e$ with $e > 3$ such that ϕ_e is absolutely irreducible.

At this point, a natural question is: what happens when ϕ_e, with e odd, is not absolutely irreducible? Using the symmetry in the variables x, y and z of the polynomial ϕ and the language of Weil divisors, we will determine all the possible divisors of the surface $\bar{X}$. This result includes the main result of [**25**] as a corollary and gives what I believe to be the limit of this kind of reasoning. With this tool, we will treat the smallest untreated example, namely $e = 5$ and confirm the correctness of the conjecture in this case.

2. The state of the art

Using the approach described in the introduction Aubry, McGuire and Rodier obtained the following results in [**1**].

THEOREM 2.1 ([**1**]). *If the degree of the polynomial function f is odd and not an exceptional number then f is not an exceptional APN function.*

THEOREM 2.2 ([**1**]). *If the degree of the polynomial function f is $2e$ with e odd and if f contains a term of odd degree, then f is not an exceptional APN function.*

There are some results in the case of Gold degree $2^i + 1$:

THEOREM 2.3 ([**1**]). *Suppose $f(x) = x^{2^i+1} + g(x)$ where $\deg(g) \leq 2^{i-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{i-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not an exceptional APN function.*

This result has been extended by Delgado and Janwa in [**11**] with the two following theorems:

THEOREM 2.4 ([**11**]). *For $k \geq 2$, let $f(x) = x^{2^i+1} + h(x) \in \mathbb{F}_q$ where $deg(h) \equiv 3 \pmod 4 < 2^i + 1$. Then f is not an exceptional APN function.*

and

THEOREM 2.5 ([**11**]). *For $k \geq 2$, let $f(x) = x^{2^i+1} + h(x) \in \mathbb{F}_q$ where $deg(h) = d \equiv 1 \pmod 4 < 2^i + 1$. If ϕ_{2^i+1} and ϕ_d are relatively prime, then f is not an exceptional APN function.*

There also exist a result for polynomials of Kasami degree $2^{2i} - 2^i + 1$:

THEOREM 2.6 ([**16**]). *Suppose $f(x) = x^{2^{2i}-2^i+1} + g(x)$ where $\deg(g) \leq 2^{2k-1} - 2^{k-1} + 1$. Let $g(x) = \sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exist a nonzero coefficient a_j of g such that $\phi_j(x, y, z)$ is absolutely irreducible. Then f is not an exceptional APN function.*

Rodier proved the following results in [**25**].

THEOREM 2.7 ([**25**]). *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be an exceptional APN function of degree $4e$ with e such that ϕ_e is absolutely irreducible. Then the polynomials of the form*

$$(x+y)(x+z)(y+z)+P,$$

with

$$P(x,y,z) = c_1\left(x^2+y^2+z^2\right) + c_4(xy+xz+zy) + b_1(x+y+z) + d_1,$$

for $c_1, c_4, b_1, d_1 \in \mathbb{F}_{q^3}$, divides ϕ.

REMARK 2.8. This theorem is originally stated for $e \equiv 3 \pmod 4$ but its proof is also valid with e such that ϕ_e is absolutely irreducible (see [**10**]).

There are more precise results for polynomials of degree 12.

THEOREM 2.9 ([**25**]). *If the degree of the polynomial f defined over $\mathbb{F}_q$ is 12, then either f is not an exceptional APN function or f is CCZ-equivalent to the Gold function x^3.*

Also, using the same approach, the present author proved the following:

THEOREM 2.10 ([**10**]). *If the degree of the polynomial f defined over $\mathbb{F}_q$ is $4e$ with $e > 3$ and such that ϕ_e is absolutely irreducible, then f is not an exceptional APN function.*

In particular, ϕ_e is absolutely irreducible when $e \equiv 3 \pmod 4$ (see lemma 4.4) so there is no exceptional APN function of degree $4e$ with $e \equiv 3 \pmod 4$.

3. New Results

The main result of this paper is:

THEOREM 3.1. *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be an exceptional APN function of degree $4e$ with e odd and let*

$$\phi(x,y,z) = \frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(y+z)(z+x)}$$

be its associated polynomial. Let σ be a generator of the Galois group $Gal(\mathbb{F}_{q^3}/\mathbb{F}_q)$. One of these three conditions holds

1. *The polynomial ϕ is divisible by*

$$(A+P(x,y,z))\left(A+\sigma\left(P(x,y,z)\right)\right)\left(A+\sigma^2\left(P(x,y,z)\right)\right),$$

   where $P(x,y,z)$ is a symmetric polynomial of degree 2 defined over $\mathbb{F}_{q^3}$.
2. *The polynomial ϕ is divisible by*

$$(\Psi(x,y,z)+L(x,y,z))\left(A\Psi(x,y,z)+R(x,y,z)\right)\sigma\left(A\Psi+R(x,y,z)\right)\sigma^2\left(A\Psi(x,y,z)+(R(x,y,z)\right),$$

   where $\Psi(x,y,z)$ is a non absolutely irreducible symmetric factor of ϕ_e defined over $\mathbb{F}_{q^3}$ but not over $\mathbb{F}_q$ and $R(x,y,z)$ and $L(x,y,z)$ are symmetric polynomials of degree respectively less than $deg(A\Psi)$ and $deg(\Psi)$ defined respectively over $\mathbb{F}_{q^3}$ and $\mathbb{F}_q$.

(3) *The polynomial ϕ is divisible by*

$$\left(A\psi^3(x,y,z)+S(x,y,z)\right)\sigma\left(A\psi^3(x,y,z)+S(x,y,z)\right)\sigma^2\left(A\psi^3(x,y,z)+S(x,y,z)\right),$$

where $\psi(x,y,z)$ is a square-free non absolutely irreducible symmetric factor of ϕ_e defined over $\mathbb{F}_{q^3}$ such that ψ, $\sigma(\psi)$ and $\sigma^2(\psi)$ are coprime.

REMARK 3.2. If ϕ_e is absolutely irreducible, then we get directly theorem 2.9 as there is clearly no polynomial satisfying the conditions (2) and (3).

In section 6, we give a direct application of the last result to the case of polynomial APN function of degree 20.

THEOREM 3.3. *Let $f:\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$ be an exceptional APN function of degree $d=20$. Then m is odd and f is CCZ-equivalent to x^5.*

4. Preliminary lemmata

We will need the following lemmas:

LEMMA 4.1. *([**25**]) The kernel of the mapping $\varpi: f\to\phi$ is made of q-affine polynomials.*

LEMMA 4.2. *([**25**]) The class of APN functions is invariant under the addition of q-affine polynomials.*

In particular, this result means that we can restrict ourselves to polynomials without any term of degree a power of 2.

LEMMA 4.3. *([**1**]) Writing $i=2^jk$ we have:*

$$\phi_i = A^{2^j-1}\phi_k^{2^j}.$$

In particular, ϕ_i is reduced if i is odd.

PROPOSITION 1. ([**18**]) The polynomial ϕ_{2^i+1} decomposes into absolutely irreducible factors as follow:

$$\phi_{2^i+1}(x,y,z)=\prod_{\alpha\in\mathbb{F}_{2^i}-\mathbb{F}_2}(x+\alpha y+(\alpha+1)z).$$

LEMMA 4.4 ([**18**]). *The polynomial ϕ_e is absolutely irreducible if $e\equiv 3 \pmod 4$.*

LEMMA 4.5 ([**1**]). *The polynomials ϕ_e and A are coprime if and only if e is odd.*

Our proof of theorem 3.1 relies on the two following propositions:

PROPOSITION 2 ([**24**]). The surface $\bar{X}$ associated to an exceptional APN function does not contain any absolutely irreducible component defined over $\mathbb{F}_q$ different from $x+y=0$, $y+z=0$ or $z+x=0$.

LEMMA 4.6 ([**1**]). *Let H be an hyperplane in $\mathbb{P}^3(\mathbb{F}_q)$. If the curve $\bar{X}\cap H$ has a reduced absolutely irreducible component defined over $\mathbb{F}_q$ then $\bar{X}$ has an absolutely irreducible component defined over $\mathbb{F}_q$.*

5. Proof of theorem 3.1

The goal of this proof is to describe how an absolutely irreducible factors of ϕ should look like under the assumption that f is an exceptional APN function. The key idea is to use lemma 4.6 along with the fact that the equation of the intersection of the surface $\bar{X}$ with the hyperplane infinity is known. For the sake of clarity, we will use the language of Weil divisors (see [**26**] for an introduction to Weil divisors) but one could directly translate this proof into terms of absolutely irreducible factors of polynomials.

Let f be an exceptional APN function of degree $d = 4e$. From proposition 2, its associated projective surface $\bar{X}$ does not contain any absolutely irreducible component defined over $\mathbb{F}_q$ excepted perhaps $x + y = 0$, $x + z = 0$ or $y + z = 0$.

Let H_∞ be the plane at infinity in $\mathbb{P}^3(\mathbb{F}_q)$ (i.e. the plane of equation $h = 0$). By lemma 4.6, the intersection $\bar{X} \cap H_\infty$ cannot contain any reduced absolutely irreducible component defined over $\mathbb{F}_q$ different from $x + y = 0$, $y + z = 0$ or $z + x = 0$. From lemma 4.3 we have:

$$\phi_d = A^3 \phi_e^4, \tag{5.1}$$

meaning that $\bar{X} \cap H_\infty$ is defined by the equation $A^3\phi_e^4 = 0$.

Let D be the divisor associated to the hyperplane section $\bar{X} \cap H_\infty$. We denote by A_0, A_1 and A_2 the divisors associated, respectively, to the section of the planes of equation $x + y = 0$, $y + z = 0$ and $z + x = 0$ with the plane H_∞. Let p_i be an absolutely irreducible factor of ϕ_e. We will denote by C_i the divisors associated to the section of the surface of equation $p_i(x, y, z) = 0$ with the plane H_∞. Then, from (5.1) and lemma 4.3:

$$D = 3(A_0 + A_1 + A_2) + 4\sum_i C_i.$$

Now let X_0 be an absolutely irreducible component of $\bar{X}$ which contains the line $x + y = 0$ in H_∞. As we have supposed that f is an exceptional APN function, X_0 is defined over an extension of $\mathbb{F}_q$, say $\mathbb{F}_{q^t}$. We choose t to be the smallest possible. Throughout this paper we will refer to σ as a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$. We set $\mathfrak{X}_0$ to be the divisor associated to the section $X_0 \cap H_\infty$, as X_0 is a component of $\bar{X}$, $\mathfrak{X}_0$ is a subdivisor of D, and as X_0 contains the line $x + y = 0$ in H_∞ we have $\mathfrak{X}_0 \geq A_0$. Our goal is to find the possible forms for $\mathfrak{X}_0$.

5.1. The case where $\mathfrak{X}_0 \geq 2A_0$.

In that case we have:

$$\mathfrak{X}_0 + \mathfrak{X}_0^\sigma \geq 4A_0.$$

But that is a contradiction since $\mathfrak{X}_0 + \mathfrak{X}_0^\sigma$ must be a subdivisor of D and D contains only three times A_0.

5.2. The case where $\mathfrak{X}_0$ contains only one time A_0.

From the previous section, we know that $\mathfrak{X}_0$ is of the form $A_0 + D_0$ where D_0 is a subdivisor of D which does not contain A_0. Thus there exists two other

absolutely irreducible components of $\bar{X}$, say X_1 and X_2, with associated divisors respectively $\mathfrak{X}_1$ and $\mathfrak{X}_2$, that contains only one time A_0.

Let G be the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$, since G fixes the line $x+y=0$ in H_∞ , the group G acts on the $\mathfrak{X}_i$ and let us consider the orbit of $\mathfrak{X}_0$ under this action. If it contains just $\mathfrak{X}_0$, then X_0 is defined over $\mathbb{F}_q$ which is impossible from proposition 2. If it contains $\mathfrak{X}_0$ and $\mathfrak{X}_1$ then G fixes $\mathfrak{X}_2$ and X_2 is then defined over $\mathbb{F}_q$, that is again in contradiction with proposition 2. Finally, that means that it contains the three components. Then G acts transitively on these three components. Let G_1 the stabilizer of X_0 . Then the group G/G_1 is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, and G_1 is the only subgroup of G of index 3. The same is true for the lines $y+z=0$ and $z+x=0$.

5.2.1. *The case* $\mathfrak{X}_0 = A_0 + \sum_i n_i C_i$.

First suppose that all the n_is are zero, hence $\mathfrak{X}_0 = A_0$ and then the equation of X_0 would be $x+y+b=0$ with $b \in \mathbb{F}_{q^t}$ and $b \notin \mathbb{F}_q$. In this case $x+y+b$ would divide $f(x)+f(y)+f(z)+f(x+y+z)$. As $b \notin \mathbb{F}_q$, by the action of G, $x+y+\sigma(b)$ would be a distinct plane containing the line $x+y=0$ in H_∞. As there are only three distinct components of $\bar{X}$ containing the line $x+y=0$ in H_∞ and as t is minimal, this implies that $t=3$. By symmetry of the variables x,y,z in the expression of $f(x)+f(y)+f(z)+f(x+y+z)$, $z+y+b$ and $x+z+b$ divide also $f(x)+f(y)+f(z)+f(x+y+z)$. Finally $f(x)+f(y)+f(z)+f(x+y+z)$ is divisible by $(x+y+b)(z+y+b)(x+z+b) = (x+y)(y+z)(z+x)+b(x^2+y^2+z^2+xy+xz+zy)+b^3$ which is of the form given in 1 in theorem 3.1.

Now suppose that there exist at least one nonzero n_i. Thus we have:

$$\mathfrak{X}_1 = A_0 + \sum_i n_i C_i^\sigma$$

and

$$\mathfrak{X}_2 = A_0 + \sum_i n_i C_i^{\sigma^2}.$$

Now suppose that $\mathfrak{X}_0$ is not invariant under the transposition (x,y), then the divisor

$$\mathfrak{X}_4 = A_0 + \sum_i n_i C_i^{(x,y)}$$

is different from the precedents and $\sum_j \mathfrak{X}_j = 4A_0 + D_1$ should be a subdivisor of D (we recall that ϕ is symmetric). That is a contradiction to the fact that D contains only three times A_0 and hence $\mathfrak{X}_0$ is invariant under (x,y).

Denote $\mathfrak{Y}_0$ (respectively $\mathfrak{Z}_0$) the image of $\mathfrak{X}_0$ by the permutation (x,y,z) (respectively (x,z,y)) and define $\mathfrak{Y}_1 = \mathfrak{Y}_0^\sigma$ and $\mathfrak{Y}_2 = \mathfrak{Y}_0^{\sigma^2}$. With the same argument as before, $\mathfrak{Y}_0$ should be invariant under (y,z), that is $\sum_i n_i C_i$ is invariant under (x,z). Thus $\sum_i n_i C_i$ (i.e. the product $\psi = \prod_i p_i(x,y,z)^{n_i}$) is symmetric.

For the sake of contradiction, suppose now that there exists an i and k such that n_k and n_i are nonzero and $C_k = C_i^\sigma$. Hence, $\mathfrak{X}_0 + \mathfrak{X}_1 + \mathfrak{Y}_0 + \mathfrak{Y}_1 + \mathfrak{Z}_0$ contains at least five times C_k which cannot happens since D contains it only four times. The same is true when we consider σ^2.

Now suppose that one of the n_i, namely n_k, is greater than 1. Then $\mathfrak{X}_0 + \mathfrak{Y}_0 + \mathfrak{Z}_0 > A_0 + A_1 + A_2 + 6C_k$, but there is only four times C_k in D because ϕ_e is reduced (see lemma 4.3), so that is a contradiction and all the n_is are maximum 1.

To summarize, $\mathfrak{X}_0$ should be of the form $A_0 + \sum_i n_i C_i$ where $n_i \leq 1$ and $\sum_i n_i C_i$ is invariant under the action of the symmetry group and does not share any common component with $\sum_i n_i C_i^{\sigma}$ or $\sum_i n_i C_i^{\sigma^2}$. By the argument of [**25**, section 5.9] (see also 5.2.3 in the present paper), we get the condition (3) of theorem 3.1.

5.2.2. *The case* $\mathfrak{X}_0 = A_0 + A_1 + \sum_i n_i C_i$.

If $\mathfrak{X}_0 = A_0 + A_1 + \sum_i n_i C_i$ we get $\mathfrak{X}_1 = A_0 + A_1 + \sum_i n_i C_i^{\sigma}$ and $\mathfrak{X}_2 = A_0 + A_1 + \sum_i n_i C_i^{\sigma^2}$. With the notations above we also have $\mathfrak{Y}_0 = A_1 + A_2 + \sum_i n_i C_i^{(x,y,z)}$. Now we just have to remark that the subdivisor of D, $\mathfrak{X}_0 + \mathfrak{X}_1 + \mathfrak{X}_2 + \mathfrak{Y}_0$ is greater than $3A_0 + 4A_1 + A_2$. That is impossible since D contains only three times A_1. Hence $\mathfrak{X}_0$ cannot be of the form $A_0 + A_1$. In the same way, we eliminate the case $\mathfrak{X}_0 = A_0 + A_2 + \sum_i n_i C_i$.

5.2.3. *The case* $\mathfrak{X}_0 = A_0 + A_1 + A_2 + \sum_i n_i C_i$.

First suppose that the n_is are all zero. That is the case 5.9 in [**25**], we copy the proof here for the sake of completeness. In this case, the equation of such X_0 is of the form $(x+y)(x+z)(y+z)+P(x,y,z)$ where P is a polynomial of degree at most 2. Let σ be a generator of G. The equation of X_1 is $(x+y)(x+z)(y+z)+\sigma(P)(x,y,z)$ and the equation of X_2 is $(x+y)(x+z)(y+z)+\sigma^2(P)(x,y,z)$. Since these polynomials are irreducible (we have supposed that X_0 is irreducible) and distinct, they are prime with each other. Therefore $f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2)$ is divisible by

$$\prod_{i=0}^{2} \left((x+y)(x+z)(y+z) + \sigma^i(P)(x,y,z)\right) \tag{5.2}$$

The equation of the curve X_∞ is

$$\left((x+y)(x+z)(y+z)\right)^3 \phi_e^4 = 0$$

so we find that the product (5.2) can contain only three summands, hence $\sigma^3(P) = P$. Hence P is defined on $\mathbb{F}_{q^3}$ and X_0 also. The product (5.2) must be symmetric in the variables x, y, z, since if it were not, the image of the product (5.2) by some element of the symmetry group $\mathbf{G}$ of the 3 variables would be different, and also divide $f(x) + f(y) + f(z) + f(x+y+z)$, therefore forcing the curve X_∞ to contain more than 3 time the line $x + y = 0$. If P is not symmetric in the variables x, y, z, then the orbit of P by the symmetry group $\mathbf{G}$ of the 3 variables would be contained in the set $\{P, \sigma(P), \sigma^2(P)\}$ since the product (5.2) is symmetric. The orbit of P under $\mathbf{G}$ is not reduced to $\{P\}$ since P is not symmetric. It is not either reduced to two elements, because the third element would be symmetric, so it is equal to the set $\{P, \sigma(P), \sigma^2(P)\}$. The stabilizer of P in $\mathbf{G}$ would then be reduced to a transposition. But the stabilizer of $\sigma(P)$ would contain a conjugate transposition, and this transposition would also fix P, as the action of $\mathbf{G}$ and G commute. So it

is impossible, which proves that P must be symmetric. Therefore P is of the form

$$P(x,y,z) = c_1(x^2+y^2+z^2) + c_4(xy+xz+zy) + b_1(x+y+z) + d_1.$$

That is the condition (1) of theorem 3.1.

So the only case left is when at least one of the n_is is non-zero. In this case we have:

$$\mathfrak{X}_1 = A_0 + A_1 + A_2 + \sum_i n_i C_i^{\sigma},$$

and

$$\mathfrak{X}_2 = A_0 + A_1 + A_2 + \sum_i n_i C_i^{\sigma^2}.$$

If $\sum_i n_i C_i$ is not invariant under the action of the symmetry group, then there exist a divisor $\mathfrak{X}_3 > A_0 + A_1 + A_2$ different from $\mathfrak{X}_0$, $\mathfrak{X}_1$ and $\mathfrak{X}_2$. Then $\sum_j \mathfrak{X}_j > D$, which is a contradiction and $\sum_i n_i C_i$ is invariant under the action of the symmetry group.

Moreover, if $\sum_i n_i C_i$ lies over $\mathbb{F}_q$ and corresponds to an absolutely irreducible factor of ϕ_i (i.e. only one of the n_i's is equal to one and all the others are zero), there exists a divisor $\mathfrak{X}_4$ which is defined over $\mathbb{F}_q$ and which contains C_i, leading again to a contradiction.

This corresponds to the condition (2) of theorem 3.1.

6. Some applications

6.1. Exceptional APN polynomials of degree 20.

In this section, we will use the theorem 3.1 to investigate the case where $e = 5$. The decomposition of ϕ_5 is given by proposition 1:

$$\phi_5 = (x + \alpha y + \alpha^2 z)(x + \alpha^2 y + \alpha z),$$

where α is in $\mathbb{F}_4 - \mathbb{F}_2$. Hence, the only symmetric factor of ϕ_5 is ϕ_5 itself and then the condition (3) of theorem 3.1 cannot hold. Also, the condition (1) is already treated in [**10**] and the conclusion is that f is CCZ-equivalent to x^5. So we only have to study the consequences of condition (2) on f. That is

$$\phi = (\phi_5 + L(x,y,z))\,(A\phi_5 + R(x,y,z))\,(A\phi_5 + \sigma\,(R(x,y,z))) \\ \left(A\phi_5 + \sigma^2\,(R(x,y,z))\right),$$

where L is a symmetrical polynomial of $\mathbb{F}_q$ of degree 1 and R is a symmetrical polynomial of $\mathbb{F}_{q^3}$ of degree 4.

The first thing we show is that $L(x,y,z) = a(x+y+z) + b = 0$. As ϕ does not have any absolutely irreducible component, $(\phi_5 + L)$ cannot be absolutely irreducible. Hence, there exist two polynomials $G(x,y,z)$ and $H(x,y,z)$ in $\bar{\mathbb{F}_2}[x,y,z]$ such that $G \times H = \phi_5 + as_1 + b$. Writing G_i and H_i the homogeneous components of degree i of G and H respectively, we get:

$$\phi_5 = G_1 \times H_1.$$

Without loss of generality we can assume that $G_1 = x + \alpha y + \alpha^2 z$ and $H_1 = x + \alpha^2 y + \alpha z$. Also,

$$a(x+y+z) = G_0(x + \alpha^2 y + \alpha z) + H_0(x + \alpha y + \alpha^2 z),$$

and hence

$$\begin{aligned} G_0 + H_0 &= a \\ G_0\alpha + H_0\alpha^2 &= a \\ G_0\alpha^2 + H_0\alpha &= a \end{aligned}$$

Plugging $G_0 = H_0 + a$ into the last two equations we get $H_0 = a\alpha$ and $H_0 = a(\alpha + 1)$, that is $a = H_0 = G_0 = 0$ and thus $b = 0$, so $L(x, y, z) = 0$.

Now, as $\phi = \sum_{j=0}^{20} a_j\phi_j$, we have for every $j = 0, \ldots, 20$, ϕ_5 divides $a_j\phi_j$. Hence

$$\phi = a_{20}\phi_{20} + a_{10}\phi_{10} + a_5\phi_5.$$

That is f is equal to $a_{20}x^{20}+a_{16}x^{16}+a_{10}x^{10}+a_8x^8+a_5x^5+a_4x^4+a_2x^2+a_1x+a_0$. As the class of APN polynomial is invariant under the addition of q-affine polynomial, we can restrict ourselves to $f = a_{20}x^{20} + a_{10}x^{10} + a_5x^5$. Clearly, f is of the form $\varphi(x^5)$ where $\varphi(x)$ is a q-affine polynomial of degree 4, hence f is EA (thus CCZ) equivalent to the polynomial x^5.

To sum up, what we proved is that the exceptional APN function of degree 20 are CCZ-equivalent to the function x^5. As this function is APN only on every extension of $\mathbb{F}_2$ of odd degree we get that m is an odd number and this concludes the proof of theorem 3.3.

6.2. Other examples.

The case $e = 9$ can be solved in the same way than the precedent one. But the impossibility of showing that $\phi_9 + L(x, y, z)$ is not absolutely irreducible if and only if L is zero leads to a long calculation which is not of real interest here but one can prove that f is CCZ-equivalent to x^9.

One can also ask if there exist e such that the condition (3) can happen. We provide an example here.

Take $e = 2^6 + 1$. Clearly, e is a Gold exponent so the decomposition of ϕ_{65} is given by proposition 1. That is

$$\phi_{65} = \prod_{\alpha \in \mathbb{F}_{2^6} - \mathbb{F}_2} (x + \alpha y + (\alpha + 1)z).$$

Now, let β be a generator of $\mathbb{F}_{2^6}$, then the polynomial

$$\begin{aligned} \psi = &(x + \beta y + (\beta + 1)z)(x + \beta^7 y + (\beta^7 + 1)z)(x + \beta^8 y + (\beta^8 + 1)z) \\ &(x + \beta^{56} y + (\beta^{56} + 1)z)(x + \beta^{55} y + (\beta^{55} + 1)z)(x + \beta^{62} y + (\beta^{62} + 1)z) \end{aligned}$$

is symmetric, defined over $\mathbb{F}_{2^3}$ (and then on $\mathbb{F}_{q^3}$) and ψ, $\sigma(\psi)$ and $\sigma^2(\psi)$ are relatively prime if $\mathbb{F}_q$ does not contain $\mathbb{F}_{2^3}$. That means that the polynomial ψ meets the condition (3) of theorem 3.1. Again, some long calculations would be necessary to investigate the consequences of this division.

In conclusion, I think that this method reaches its limit here and I would suggest to try a different approach to solve the remaining cases.

References

[1] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, Finite Fields Theory and applications, Ninth International conference Finite Fields and Applications, McGu & al.editors, Contemporary Math. n°518, AMS, Providence (RI), USA, 2010, pp23-31.

[2] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4160-4170.

[3] Biham, E. and A. Shamir. (1990). Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology CRYPTO '90. Springer-Verlag. 221.

[4] N. Bourbaki, Élments de mathé matique, Algèbre. Springer-Verlag Berlin Heidelberg 2007

[5] Browning, K. A.; Dillon, J. F.; McQuistan, M. T.; Wolfe, A. J. An APN permutation in dimension six. Finite fields: theory and applications, 3342, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[6] L. Budaghyan and C. Carlet and P. Felke and G. Leander An infinite class of quadratic APN functions which are not equivalent to power mappings, Cryptology ePrint Archive, n° 2005/359.

[7] Byrne E. and McGuire G., Quadratic Binomial APN Functions and Absolutely Irreducible Polynomials, eprint arXiv:0810.4523 [math.NT].

[8] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like crypto-systems. Designs, Codes and Cryptography, 15(2), pp. 125-156, 1998.

[9] F. Caullery, Polynomial functions of degree 20 which are not APN infinitely often. eprint arXiv:1212.4638.

[10] F. Caullery, The exceptional APN functions of degree $4e$. eprint arXiv:1309.7776

[11] M. Delgado, H. Janwa, On the Conjecture on APN Functions, eprint arXiv:1207.5528

[12] J. Dillon, APN Polynomials: An Update. Fq9, International Conference on Finite Fields and their Applications July 2009.

[13] Dobbertin, Hans; Mills, Donald; Muller, Eva Nuria; Pott, Alexander; Willems, Wolfgang; APN functions in odd characteristic. Combinatorics 2000 (Gaeta). Discrete Math. 267 (2003), no. 1-3, 95112.

[14] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52 (2006), no. 2, 744-747.

[15] Y. Edel, A. Pott. A new almost perfect nonlinear function which is not quadratic Adv. Math. Commun.3 (2009), no. 1, 59-81.

[16] E. Ferard, R. Oyono and F. Rodier. Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents. accepted in Proceedings of AGCT 13, March 2012.

[17] Hernando, Fernando; McGuire, Gary Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. J. Algebra 343 (2011), 7892.

[18] H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-10 (G Cohen, T. Mora and O. Moreno Eds.), 180-194, Lecture Notes in Computer Science, Vol. 673, Springer-Verlag, New York/Berlin 1993.

[19] E. Leducq, New families of APN functions in characteristic 3 or 5, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, AMS, 2012, 574, 115-123.

[20] G. Leander and F. Rodier Bounds on the degree of APN Polynomials. The case of $x^{-1}+g(x)$. Designs, Codes and cryptography. 0925-1022. 2009.

[21] Ness, Geir Jarle; Helleseth, Tor A new family of ternary almost perfect nonlinear mappings. IEEE Trans. Inform. Theory 53 (2007), no. 7, 25812586.

[22] K. Nyberg, Differentially uniform mappings for cryptography, Advances in cryptology-Eurocrypt '93 (Lofthus, 1993), 55-64, Lecture Notes in Comput. Sci., VOl. 765, Springer, Berlin, 1994.

[23] Poinsot, Laurent; Pott, Alexander Non-Boolean almost perfect nonlinear functions on non-Abelian groups. Internat. J. Found. Comput. Sci. 22 (2011), no. 6, 13511367.

[24] F. Rodier, Borne sur le degré des polynômes presque parfaitement non-linéaires. Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman editors, Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169-181, 2009.

[25] F. Rodier, Functions of degree 4e that are not APN infinitely often. Cryptogr. Commun. 3 (2011), n°4, 227-240.

[26] Shafarevich, I.R., Basic Algebraic Geometry, Vol. 1. 1994, Springer-Verlag.
[27] Zha, ZhengBang; Wang, XueLi; Power functions with low uniformity on odd characteristic nite elds. Sci. China Math. 53 (2010), no. 8, 19311940.1869-1862.
[28] Zha, Zhengbang; Wang, Xueli; Almost perfect nonlinear power functions in odd characteristic. IEEE Trans. Inform. Theory 57 (2011), no. 7, 48264832.1557-9654.

Institut Mathmatique de Marseille, CNRS, Marseille, France
Current address: Institut Mathmatique de Marseille, CNRS, Marseille, France
E-mail address: florian.caullery@univ-amu.fr